

МИНОБРНАУКИ РОССИИ

**Федеральное государственное бюджетное образовательное учреждение**

**высшего образования**

**«Казанский национальный исследовательский технологический университет»**

**(ФГБОУ ВО «КНИТУ»)**

Кафедра\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Направление\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Специальность\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Группа\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

**ВЫПУСКНАЯ КВАЛИФИКАЦИОННАЯ РАБОТА**

Уровень образования\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

(бакалавр, специалист, магистр)

Вид ВКР\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

( проектный, исследовательский, комбинированный)

Тема\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_

Рецензент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Зав. кафедрой\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Нормоконтролер\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Руководитель\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Студент\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_(\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Консультанты:

по экономической части\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

по безопасности и экологии\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

по автоматизации производства

и метрологии\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

по патентной части\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

по библиографии\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_ (\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_\_)

Казань 2017

[**Введение** 5](#_Toc472625483)

[**1.** **История случайных чисел** 7](#_Toc472625484)

[1.1. Древний мир. 7](#_Toc472625485)

[1.2. Случайность в политике. 8](#_Toc472625486)

[1.3. Новое время. 8](#_Toc472625487)

[1.4. Новейшее время. 9](#_Toc472625488)

[1.5. Случайные и псевдослучайные числа 10](#_Toc472625489)

[1.6. Генераторы случайных чисел. 11](#_Toc472625490)

[1.7. Биологические датчики псевдослучайных чисел 13](#_Toc472625491)

[**2.** **Разработка программы для генерации псевдослучайных чисел с помощью биометрических параметров.** 17](#_Toc472625492)

[*2.1.* Выбор языка программирования для написания программы 17](#_Toc472625493)

[*2.2.* Архитектура программы 17](#_Toc472625494)

[*2.3.* Класс-форма MainForm 18](#_Toc472625495)

[*2.4.* Класс-форма RNGBUTTONSForm 19](#_Toc472625496)

[*2.5.* Класс-форма BRNGKeyForm 21](#_Toc472625497)

[*2.6.* Класс-форма BRNGMOUSEForm. 23](#_Toc472625498)

[**Заключение** 25](#_Toc472625499)

[**Cписок источников** 26](#_Toc472625500)

[**Приложения** 27](#_Toc472625501)

# **Введение**

Современный мир завязан на случайных числах. Они используются во многих сферах, таких как: наука, игры, статистика, криптография, искусство. Например, ученые проводят рандомизированные контролируемые испытания - это такой тип научного (часто медицинского) эксперимента, при котором его участники случайным образам делятся на группы, в одной из которых проводится исследуемое вмешательство, а в другой (контрольной) применяются стандартные методики или плацебо, а генераторы случайных и псевдослучайных чисел используются во многих компьютерных играх.

Для каждой области использования случайных чисел существуют определённые требования, удовлетворить которым могут специально подобранные методы. С точки зрения математики следует разделять случайные и псевдослучайные числа и способы их генерации, а значит, и области применения. Например, применение в криптографии, как правило, имеет жесткие требования, в то время как в других видах использования, где случайность не так важна, можно использовать более свободный стандарт псевдослучайности.

Одним из подходов к генерации последовательности чисел является использование биологических генераторов случайных чисел. Главной его особенностью является использование случайности биометрических данных (после их приведения в числовую систему) как начальную последовательность для псевдослучайных генераторов или непосредственно как случайную последовательность чисел. Это может иметь практическую значимость для генерации «ключа сессии» в таких протоколах как SSL, SSH, PGP или SET. Так же биологический датчик может стать заменой для программных генераторов случайных чисел, основанных на системном времени или содержимом буфера, в виду большей устойчивости к атакам злоумышленников.

Генераторы случайных чисел могут реализованы программно, либо аппаратно. Программная реализация подразумевает использование математических алгоритмов, результатом работы которых является статистически независимая последовательность чисел, соответствующая равномерному распределению. Стоит отметить что такая последовательность является детерминированной, так как получена из начального значения по определенному алгоритму. Следовательно, любая реализация подобного генератора принадлежит к категории псевдослучайных из-за своей детерминированности.

В связи с вышеизложенным можно сказать, что выбранная нами тема является важной частью криптографии в целом и в подходах генерации случайных чисел, в частности.

Целью данной работы является программная реализация биологического генератора случайных чисел. В теоретической части нами будут рассмотрены такие понятия, как случайные и псевдослучайные числа, случайность, биологические датчики генерации случайных чисел и подходы к их реализации, а также алгоритмы, которые будут использованы при написании программы. применение этих чисел и методы их генерации.

Поставлены следующие задачи:

* Рассмотреть понятия случайных и псевдослучайных чисел.
* Изучить концепцию биологических датчиков случайных чисел.
* Реализовать программно биологический датчик случайных чисел.

Работа состоит из двух глав, введения, заключения, списка использованной литературы и приложения.

# **История случайных чисел**

## 1.1. Древний мир.

Развитие понятия случайности в ходе истории человечества было крайне неравномерным. Историки часто задаются вопросом, почему прогресс развития данного концепта был таким медленным, учитывая, что люди сталкивались с ним испокон веков? Некоторые ученые считают, что среднестатистический человек той эпохи не был заинтересован в изучении и осмыслении случайности.

В древней истории концепция случайности и «шанса» были тесно завязаны на судьбе. В ту эпоху многие народы бросали гадальные кости чтобы предсказать судьбу, позже это переросло в разнообразные азартные игры. Свидетельства распространения таких игр находят в древнем Египте, Индии и Китае.

По всей видимости, первыми, кто формализовал случайности, были китайцы. Так, в одном из наиболее ранних китайских философских трудов «Книга перемен» рассматривалось гадание при помощи довольно сложных псевдослучайных процедур, использующих монеты или веточки тысячелистника, шести черт и поиска в книге соответствующей гексаграммы. Два основополагающих элемента китайской философии, инь и ян, были в «Книге перемен» скомбинированы в различных формах, чтобы продуцировать знакомую всем игру «*орел или решка».*

На Западе же, первыми, кто описывал случайность, были греки. Около 400 века до н.э греческий философ Демокрит представил свое предположение о мире, управляемом единообразующим законом мироздания, а случайность определил, как неспособность человека понять истинную природу некоторых событий. **[1]**

Так или иначе, до 16 века мир был сфокусирован на нематематическом аспекте случайности.

## 1.2. Случайность в политике.

Случайность имела и продолжает иметь место и в политической жизни человечества. Древнегреческая демократия в своем первоначальном состоянии предполагала власть народа, и многие руководящие должности выбирались случайным образом при помощи жребия. Такое распределение должностей позволяло избежать коррупции и концентрации власти у одной определенной ячейки общества.

В настоящее время выборы при помощи жребия ограничены, и используются главным образом в отборе [присяжных заседателей](https://ru.wikipedia.org/wiki/%D0%9F%D1%80%D0%B8%D1%81%D1%8F%D0%B6%D0%BD%D1%8B%D0%B9_%D0%B7%D0%B0%D1%81%D0%B5%D0%B4%D0%B0%D1%82%D0%B5%D0%BB%D1%8C) в англо-саксонской правовой системе в [Великобритании](https://ru.wikipedia.org/wiki/%D0%92%D0%B5%D0%BB%D0%B8%D0%BA%D0%BE%D0%B1%D1%80%D0%B8%D1%82%D0%B0%D0%BD%D0%B8%D1%8F) и [США](https://ru.wikipedia.org/wiki/%D0%A1%D0%BE%D0%B5%D0%B4%D0%B8%D0%BD%D1%91%D0%BD%D0%BD%D1%8B%D0%B5_%D0%A8%D1%82%D0%B0%D1%82%D1%8B_%D0%90%D0%BC%D0%B5%D1%80%D0%B8%D0%BA%D0%B8). Некоторые страны, например, Ирак, тоже пытаются перенять данную практику, так как это положительно влияет на беспристрастность присяжных.

## 1.3. Новое время.

Примерно в 1620 году Галилео Галилей написал «Рассуждение об игре в кости», где он довольно подробно проанализировал эту задачу. В 1654 году, сподвигнутые интересом Антуана Гомбо к азартным играм, Блез Паскаль и Пьер Ферма проделали большую работу, чтобы положить основы для развития теории вероятности. «Пари Паскаля» отмечается как раннее использование понятия бесконечности и первое формальное использование теории вероятности. Работа Паскаля и Ферма повлияли в свою очередь на работу Лейбница и его «математический анализ», который в свою очередь способствовал дальнейшему пониманию вероятности и случайности.

В то время как математические гении той эпохи закладывали фундамент в современное понимание случайности, общество в своем большинстве продолжало полагаться на случайность во всевозможных предсказаниях и гаданиях.

Термин энтропия был предложен великим немецким ученым Рудольфом Клаузиусом в его труде «О различных удобных для применения формах второго начала математической теории теплоты», в котором было введено важнейшее для понимания случайности понятие [энтропии](https://ru.wikipedia.org/wiki/%D0%AD%D0%BD%D1%82%D1%80%D0%BE%D0%BF%D0%B8%D1%8F).

## 1.4. Новейшее время.

В течение 20 века четыре главные интерпретации вероятности были хорошо изучены и поняты (рис. 1):

|  |  |  |  |  |
| --- | --- | --- | --- | --- |
|  | **Классическая** | **Частотная** | **Субъективная** | **Свойственная** |
| **Главная гипотеза** | Принцип равноценности | Частота появления | Степень доверия | Степень детерминированных связей |
| **Концептуальный базис** | Гипотетическая симметрия | Предыдущие данные о системе | Знания и интуиция | Нынешнее состояние системы |
| **Концептуальный подход** | Гипотетический | Эмпирический | Субъективный | Метафизический |
| **Проблемы** | Противоречия в принципе равноценности | Цикличные определения | Проблема назначения классов | Спорная концепция |

Рис. 1. Классификация интерпретаций вероятности.

В это время случайные числа и случайность нашли применение во многих прикладных сферах, таких как финансы и физика. В 1900 году французский математик Л.Башелье при помощи Броуновского движения попытался описать финансовые опционы, что послужило основой развития финансовой математики и стохастических процессов.

Развитие квантовой механики в начале 20го века и формулирование принципа неопределённости Гейзенбе́рга в 1927 году положили конец Ньютоновскому мышлению среди физиков относительно определённости природы.

В 1948 году Клод Шеннон разработал информационную теорию, которая дала толчок энтропическому взгляду на случайность.

## 1.5. Случайные и псевдослучайные числа

  Случайные числа – это такая последовательность чисел, в которой невозможно предугадать следующее число, даже зная всю числовую последовательность. Псевдослучайные числа – это последовательность чисел, имеющая признаки случайных чисел, но каждое следующее число вычисляется по специально подобранному алгоритму. Несомненным преимуществом псевдослучайных чисел является их быстрая генерация и отсутствие необходимости в специальных аппаратных устройствах, но есть и существенный недостаток – запас псевдослучайных чисел ограничен.

В свою очередь, алгоритм, результатом выполнения которого является последовательность псевдослучайных чисел, называется генератором псевдослучайных чисел.

Стоит отметить, что имеет смысл генерировать псевдослучайные числа только с равномерным законом распределения, так как все остальные можно получить из равномерного распределения путём преобразований, известных из теории вероятности.

В свою очередь, равномерным называется такое распределение, при котором случайная величина имеет конечное количество равновероятных значений. Существует классический пример из теории вероятности. Пусть дана последовательность, состоящая из нулей и единиц, вероятность появления нуля в данной последовательности в среднем будет равна 50%. Но это не означает, что в последовательности длиной в 1000 цифр будет 500 нулей. Более того, в такой последовательности может быть 999 единиц, а вероятность того, что тысячным элементом будет нуль, так же составляет 50%. При рассмотрении же достаточно большой последовательности нули будут встречаться в половине случаев. Это утверждение кажется большинству парадоксальным, однако оно не противоречит реальности.

## 1.6. Генераторы случайных чисел.

В те времена, когда еще не были изобретены компьютеры, случайные числа получали довольно варварским способом, вытягивая карты, вытаскивая разноцветные шары из мешков, бросая кости. Совершенно очевидно, что данные методы были далеки от совершенства, поэтому в 1927 году Л.Х.К. Типпетт разработал и опубликовал первую таблицу случайных чисел.

С развитием науки и технологий количество необходимых случайных чисел росло, тогда стали появляться машины, генерирующие случайные числа. Первая такая машина была использованная в 1939 году М.Ж. Кендаллом и Б. Бабингтон-Смитом для построения таблицы, содержащей 100 000 случайных чисел. Корпорация RAND при помощи таких устройств сгенерировала и опубликовала таблицу, состоящую из миллиона случайных чисел. Так же стоит упомянуть генератор случайных чисел ERNIE, применявшийся в течении многих лет в Великобритании для генерации номеров выигравших билетов лотереи. В наши дни, эти устройства тоже имеют применение, являясь генераторами энтропии. Такие генераторы способны генерировать истинные случайные числа, но у них есть существенный недостаток – цена. Именно поэтому и возникла необходимость в генераторах псевдослучайных чисел. **[2]**

После изобретения компьютеров начались исследования эффективного способа получения случайных чисел, встроенных программно в компьютеры. В начале применение таблиц было малоэффективным, так как из-за ограниченности памяти на заре появления компьютеров и необходимости ручного ввода таблицы не могли быть слишком большими. Технологический прогресс позволил вернуться к использованию таблиц в 90-е годы, миллиарды тестированных случайных байтов можно было разместить на таких носителях, как компакт диск. В 1995 году Дж. Марсалья подготовил демонстрационный диск с 650 мегабайтами случайных чисел, при генерировании которых запись шума диодной цепи сочеталась с определенно скомпонованной музыкой в стиле рэп. Сам Марсалья называл это белым и черным шумом. **[3]**

Несовершенство первых механических методов побудило к созданию генераторов псевдослучайных чисел при помощи арифметических операций, заложенных в компьютер. Одним из первых, около 1949 года, такой генератор предложил Джон фон Нейман. Данный метод получил название метода середины квадрата, его суть заключается в следующем: нужно возвести предыдущее случайное число в квадрат, а затем выделить средние цифры. Данный метод долго использовался для генерации случайных чисел, несмотря на то, что к нему было множество претензий.

Так же свой метод предлагал и Дональд Кнут, назвав его «супергенератор случайных чисел», его суть можно описать следующей последовательностью шагов:

К1. [Выбрать число итераций.] Присвоить Y наибольшую значащую цифру Х. (Мы выполним шаги К2-К13 точно Y+1 раз, т. е. применим рандомизированные преобразования случайное число раз.)

К2. [Выбрать случайный шаг] Присвоить следующую наибольшую значащую цифру X. Переходим к шагу К (3 + Z), т. е. к случайно выбранному шагу в программе.

КЗ. [Обеспечить> 5 х 109] Если X <5000000000, присвоить X значение X + 5000000000.

К4. [Средина квадрата.] Заменить X серединой квадрата X.

К5. [Умножить.] Заменить X числом (1001001001 X) mod 1010.

К6. [Псевдодополнение.] Если X <100000000, то присвоить X значение X + 9814055677; иначе присвоить X значение 1010- X.

К7. [Переставить половины.] Поменять местами пять младших по порядку знаков со старшими.

К8. [Умножить.] Выполнить шаг К5.

К9. [Уменьшить цифры.] Уменьшить каждую не равную нулю цифру десятичного представления числа X на единицу.

К10. [Модифицировать на 99999.] Если А' <105, присвоить X значение — X 2 +99999; иначе присвоить X значение X — 99999.

К11. [Нормировать.] (На этом шаге А' не может быть равным нулю.) Если X <109, то умножить X на 10.

К12. [Модификация метода средин квадратов.] Заменить Х на средние 10 цифр числа Х (Х — 1).

К13. [Повторить?] Если Y> 0, уменьшить У на 1 и возвратиться к шагу К2. Если Y = 0, алгоритм завершен. Значение числа X, полученное на предыдущем шаге, и будет желаемым «случайным» значением. **[4]**

После рассмотрения всех преобразований алгоритма К кажется правдоподобным, что можно было бы обеспечить бесконечное количество случайных числе. На самом деле, когда этот алгоритм впервые был реализован на компьютере, он почти мгновенно сошелся к 10-значному числу 6065038420, которое преобразовывалось само в себя.

Так же стоит упомянуть линейный конгруэнтный метод. Данную схему предложил Д. Г. Лехмер в 1949 году. Суть этого метода описывается формулой: **[5]**

**Ki = (A \* Ki-1 + C) mod M, I ≤ 0.**

где Ki следующее случайное число;

Ki-1 -предыдущее псевдослучайное число;

A, C, M – некоторые константы.

Например, при M = 2, а Кi-1=A=C=4 получим последовательность 4, 10, 12, 26, 54…

Данный метод находит широкое применение в стандартных библиотеках многих компиляторов, и, хотя исследования показывают, что он способен генерировать хорошую последовательность псевдослучайных чисел, его криптографическая стойкость невелика.

## 1.7. Биологические датчики псевдослучайных чисел

В данной работе будет рассмотрено несколько алгоритмов, которые позволяют программно реализовать биологический датчик случайных чисел.

Смысл данного генератора состоит в использовании биологических параметров человека, после их преобразования в числовое представление. Источником энтропии в подобных генераторах могут выступать различные биологические данные, такие как скорость реакции пользователя на различные события, рисунок отпечатка пальца, радужка глаза, скорость расщепления определенных ферментов и т.п. У таких метода есть свои преимущества, среди которых можно выделить отсутствие необходимости дополнительного оборудования, простоту использования. Данный генератор в реализации компании КриптоПро сертифицирован для генерации ключей КС1. Среди минусов стоит упомянуть время генерации, которое намного больше, чем генерация другими алгоритмами генерации псевдослучайных чисел.

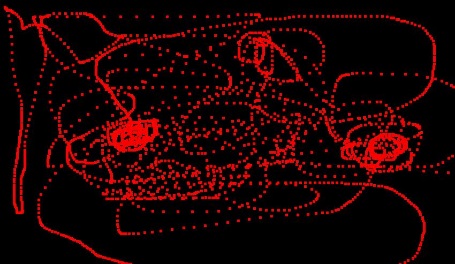
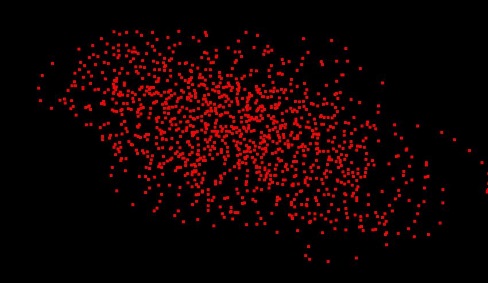
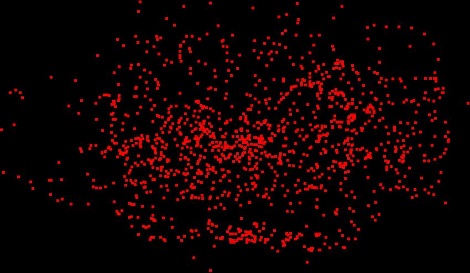
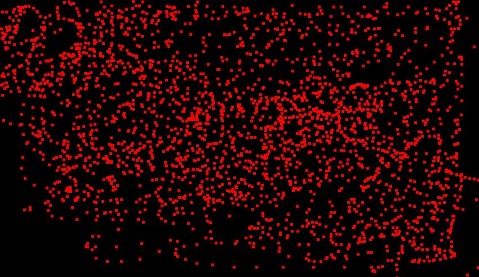
### 1.8. Генерация случайных чисел, основанная на движении мыши

Как говорилось ранее, биологические генераторы случайных чисел позволяют получать хорошие последовательности, но при реализации подобного генератора на персональном компьютере, что может быть не детерминированным источником? Существует множество подходящих явлений, таких как температурный шум, атмосферный шум, период полураспада радиоактивных элементов или даже просто подбрасывание монетки. Все эти методы позволяют так или иначе получить случайные числа, но при попытке их использования на ПК, возникает несколько проблем, эти методы либо слишком дороги для использования обычными пользователями, мало кто имеет доступ к радиоактивным элементам, либо слишком медлительны, например, представьте сколько потребуется времени для генерации 1000 чисел при подбрасывании монетки. В большинстве случаев подобные недетерминированные источники требуют дополнительные аппаратные средства, что делает их использование не таким распространенным.

Другое дело компьютерная мышь, она имеется практически у каждого пользователя персонального компьютера, скорость генерации чисел приемлема и от пользователя не требуется особых знаний или умений.

По своей сути движение мыши — это физическое движение и генерирует аналоговые сигнал, в то время как ПК работает с цифровыми. В связи с этим необходима конвертация аналоговых сигналов в цифровые, к счастью для нас практически все операционные системы уже сделали это для нас. При вызове имеющихся API (application programming interface), которые реализованы для каждой из популярных операционных систем, мы можем получать координаты движения мыши. Значения этих координат обычно находятся в диапазоне от одного до нескольких тысяч. Для облегчения использования этих данных в наших экспериментах, мы будем линейно приводить их к диапазону от 1 до 64. Таким образом, движение мыши может быть смоделировано как изображении 64x64 после аналого-цифрового преобразования.

При использовании движения мыши как источника энтропии стоит отметить, что существуют определенные шаблоны движения мыши для одного пользователя. Другими словами, существует некоторая закономерность движения мыши в разные моменты времени для одного и того же пользователя. Соответственно разные пользователи могут иметь разные шаблоны. (Рис. 2)



В связи с шаблоннизированностью разных вводов от одного и того же пользователя, мы должны осторожно обрабатывать эти данные. Другими словами, сгенерированная последовательность может быть так же похожа для одного и того же пользователя. Чтобы преодолеть этот недостаток, нужно сделать так, чтобы результат после обработки входных данных был очень чувствителен к изменению этих данных.

### 1.10. Оценка случайности чисел

На сегодняшний день существуют множество подходов к оценке случайности последовательности чисел.

# **2. Разработка программы для генерации псевдослучайных чисел с помощью биометрических параметров.**

## Выбор языка программирования для написания программы

На сегодняшний день, существует множество языков программирования, каждый из которых придерживается определенной парадигмы. Из всего спектра парадигм мы бы хотели выделить объектно-ориентированное программирование, которое позволяет не задумываться над низкоуровневыми процессами и сосредоточиться на архитектуре и классах.

Выбирая язык для реализации данной программы, были учтены следующие критерии: язык

1. Должен быть объектно-ориентированным;
2. Должен быть прост в изучении;
3. Должен иметь удобную среду разработки;
4. Должен компилироваться на ОС Windows;
5. Должен предоставлять удобные инструменты для реализации

программы.

Исходя из всего этого, был выбран язык программирования C#, который является мощным ООП языком, разработанным Microsoft в начале 2000-х годов для разработки на платформе .Net. **[6]**

## Архитектура программы

Программа реализована как win form приложение и по существу разбита на несколько классов-форм.

1. **MainForm** – это стартовая форма, позволяющая осуществлять навигацию по приложению;
2. **RNGBUTTONSForm** – это форма для генерации случайных чисел при нажатии на кнопку;
3. **RNGKEYForm** – это форма для генерации случайных чисел по нажатию определённых клавиш на клавиатуре;
4. **RNGMOUSEForm** – это форма для генерации случайных чисел при передвижении курсора мыши в определенной области.

## Класс-форма MainForm

Данная форма позволяет переключаться между различными способами генерации случайных чисел, представленных в программе. На этой форме есть четыре элемента, три «кнопки» для перехода между формами и один «TextBox» для хранения и представления сгенерированных чисел (см. Приложение А).

Для начала происходит инициализация компонентов формы.

public partial class MainForm : Form

{

public MainForm()

{

InitializeComponent();

}

Теперь рассмотрим методы, содержащиеся в данном классе.

private void GenerateByButtonsButton\_Click(object sender, EventArgs e)

{

this.Hide();

BRNGForm numberGenerator = new BRNGForm(this);

numberGenerator.Show();

}

Данный метод вызывается при нажатии на кнопку «**Generate By Button**» в **MainForm.** В этом методе создается экземпляр класса **BRNGForm**, отправляя как параметр конструктора экземпляр **MainForm** для того, чтобы можно было обратно вывести эту же форму при завершении генерации. Далее вызывается метод **Show** на этом экземпляре, который является наследуемым от базового класса **Form**.

private void GenerateByLettersButton\_Click(object sender, EventArgs e)

{

this.Hide();

BRNG.Forms.BRNGKeyForm numberGeneratorByKeys = new Forms.BRNGKeyForm(this);

numberGeneratorByKeys.Show();

}

Данный метод вызывается при нажатии на кнопку «**Generate By Letters**» в **MainForm.** В этом методе создается экземпляр класса **BRNGKeyForm**, отправляя как параметр конструктора экземпляр **MainForm** для того, чтобы можно было обратно вывести эту же форму, и вызывает метод **Show** на это экземпляре, который является наследуемым от базового класса **Form**.

private void GenerateByMouseButton\_Click(object sender, EventArgs e)

{

this.Hide();

BRNG.Forms.BRNGMOUSEForm numberGeneratorByMouse = new Forms.BRNGMOUSEForm(this);

numberGeneratorByMouse.Show();

}

Данный метод вызывается при нажатии на кнопку «**Generate By Mouse**» в **MainForm.** В этом методе создается экземпляр класса **BRNGMOUSEForm**, отправляя как параметр конструктора **MainForm** для того, чтобы можно было обратно вывести эту же форму, и вызывает метод **Show** на этом экземпляре, который является наследуемым от базового класса **Form**.

public void CheckResultOfGeneration(bool result)

{

if (!result)

{

MessageBox.Show("Unsuccessful atempt of generation.", "Warning", MessageBoxButtons.OK, MessageBoxIcon.Warning);

}

}

}

Последний метод вызывается для оповещения пользователя в случае неуспешной генерации последовательности.

## Класс-форма RNGBUTTONSForm

Данный класс-форма вызывается при нажатии на кнопку **«Generate By Button»** на главной форме. На форме присутствует одна кнопка, которая меняет свое местоположение на форме при нажатии на нее (см. Приложение Б). Рассмотрим структуру более подробно.

public partial class BRNGForm : Form

{

private int counter = 0;

Engine.RandomPointGeneratorEngine Point;

Stopwatch entropy;

MainForm previousForm;

Сначала объявим необходимые поля:

1. Целочисленное поле **Counter** для подсчета нажатий на кнопку;
2. Экземпляр класса **RandomPointGeneratorEngine** **Point** для задания положения кнопки;
3. Экземпляр класса **Stopwatch** **Entropy** для отсчета времени между нажатиями на кнопку, **которое** и будет псевдослучайным числом;
4. Экземпляр класса **MainForm PreviousForm** для хранения предыдущей формы и возможности возврата к ней.

public BRNGForm(MainForm form)

{

InitializeComponent();

entropy = new Stopwatch();

previousForm = form;

Point = new Engine.RandomPointGeneratorEngine();

entropy.Start();

}

В конструкторе данного класса инициализируем все поля, описанные выше.

private void BRNGPicture\_Click(object sender, EventArgs e)

{

entropy.Stop();

if (counter < 10)

{

previousForm.mainRichTextBox.AppendText((entropy.ElapsedMilliseconds).ToString() + " ");

counter++;

BRNGPicture.Location = Point.GenerateNewPoint(this.Size.Height, this.Size.Width);

entropy.Reset();

entropy.Start();

}

else

{

this.Close();

previousForm.Show();

}

}

Данный метод **BRNGPicture\_Click** является обработчиком события при нажатии на кнопку **BRNGPicture,**  и вызывается при каждом нажатии. После нажатия на кнопку **entopy** прекращается отсчет времени и проверяется условие. Если количество нажатий не превышает десять, тогда в **mainRichTextBox,** находящийся на предыдущей форме, мы отправляем количество миллисекунд, прошедших между нажатиями на кнопку, сбрасываем секундомер **entropy** и запускаем его снова. Если же количество нажатий на кнопку не меньше десяти, тогда мы закрываем эту форму и выводим предыдущую.

private void BRNGForm\_Load(object sender, EventArgs e)

{

MessageBox.Show("Click on picture of plane to generate random numbers .", "Info", MessageBoxButtons.OK, MessageBoxIcon.Information);

}

Данный метод **BRNGForm\_Load** является обработчиком события загрузки формы **BRNGForm** и вызывается при ее загрузке. Он выводит на экран сообщение о работе данного метода генерации и не влияет на работу программы.

private void BRNGForm\_FormClosed(object sender, FormClosedEventArgs e)

{

previousForm.Show();

}

Данный метод **BRNGForm\_FormClose** является обработчиком события закрытия формы **BRNGForm** и вызывается при ее закрытии пользователем, для того чтобы вывести предыдущую форму.

## Класс-форма BRNGKeyForm

Данный класс-форма вызывается при нажатии на кнопку **«Generate By Letters»** на главной форме. На форме присутствует счетчик ошибок и оставшихся итераций генерирования случайного числа и буквы, которя будет менять свое местоположение и значение при нажатии соответствующей клавиши на клавиатуре (см. Приложение В).

public partial class BRNGKeyForm : Form

{

private MainForm previousForm;

private int lettersCounter = 0;

private int errorsCounter = 0;

Engine.RandomPointGeneratorEngine newChar;

System.Diagnostics.Stopwatch entropy;

Сначала объявим необходимые поля:

1. Целочисленное поле **lettersCounter** для подсчета правильных нажатий клавиши;
2. Целочисленное поле **errorsCounter** для подсчета ошибочных нажатий клавиши;
3. Экземпляр класса **RandomPointGeneratorEngine** **newChar** для генерации новой буквы;
4. Экземпляр класса **Stopwatch** **Entropy** для отсчета времени между нажатиями на кнопку, **которое** и будет псевдослучайным числом;
5. Экземпляр класса **MainForm PreviousForm** для хранения предыдущей форма и возможности возврата к ней.

public BRNGKeyForm(MainForm \_previusForm)

{

newChar = new Engine.RandomPointGeneratorEngine();

previousForm = \_previusForm;

InitializeComponent();

entropy = new System.Diagnostics.Stopwatch();

entropy.Start();

lettersLeftLabel.Text = "9";

errorsLabel.Text = "0";

}

В конструкторе происходит инициализация всех полей.

private void BRNG\_KeyPress(object sender, KeyPressEventArgs e)

{

if (keyFormLabel.Text == e.KeyChar.ToString().ToUpper())

{

lettersCounter++;

lettersLeftLabel.Text = (Convert.ToInt32(lettersLeftLabel.Text) - 1).ToString();

entropy.Stop();

previousForm.mainRichTextBox.AppendText(entropy.ElapsedMilliseconds.ToString() + " ");

keyFormLabel.Text = newChar.GenerateNewChar().ToString();

entropy.Reset();

entropy.Start();

keyFormLabel.Location = newChar.GenerateNewPoint(this.Size.Height, this.Size.Width);

}

else

{

errorsCounter++;

lettersCounter--;

if (lettersCounter < 0)

{

MessageBox.Show("Too much errors!", "Warning", MessageBoxButtons.OK, MessageBoxIcon.Error);

previousForm.mainRichTextBox.Clear();

previousForm.CheckResultOfGeneration(false);

previousForm.Show();

this.Close();

return;

}

errorsLabel.Text = errorsCounter.ToString();

lettersLeftLabel.Text = (Convert.ToInt32(lettersLeftLabel.Text)).ToString();

}

if (lettersCounter > 9)

{

previousForm.Show();

this.Close();

}

}

Теперь рассмотрим сам метод генерации псевдослучайной последовательности. При загрузке формы в окне появляется буква, задача пользователя нажать соответствующую клавишу на клавиатуре. Метод **BRNG\_KeyPress** срабатывает при нажатии пользователем на любую клавишу клавиатуры, далее идет проверка соответствия нажатой клавиши запрашиваемому символу, и если все верно, то мы обновляем счетчик оставшихся нажатий, а также останавливаем секундомер и отправляем на **MainForm** сгенерированное число. Далее идет перезапуск таймера и генерация нового местоположения для символа, так же, как и самого символа. Если же пользователь совершает ошибку, то увеличивается количество ошибок и уменьшается количество успешных нажатий. При достижении количества успешных нажатий отрицательного значения, пользователя предупредят об ошибке при генерации псевдослучайных чисел.

private void BRNGKeyForm\_Load(object sender, EventArgs e)

{

MessageBox.Show("Press letters showed on the screen to generate random numbers .", "Info", MessageBoxButtons.OK, MessageBoxIcon.Information);

}

Последний метод делает то же, что и в предыдущих формах: они показывают сообщение с описанием работы выбранного биологического генератора случайных чисел.

## Класс-форма BRNGMOUSEForm.

Данный класс-форма вызывается при нажатии на кнопку **«Generate By Mouse»** на главной форме. На форме поле для генерации псевдослучайных чисел и шкала для отсчета сгенерированных чисел (см. Приложение Г).

public partial class BRNGMOUSEForm : Form

{

private MainForm previusForm;

private Stopwatch controler;

private int counter;

public BRNGMOUSEForm(MainForm \_PreviusForm)

{

previusForm = \_PreviusForm;

InitializeComponent();

controler = new Stopwatch();

controler.Start();

}

В начале как обычно объявляем поля и инициализируем их в конструкторе.

private void mouseFormPictureBox\_MouseMove(object sender, MouseEventArgs e)

{

if (controler.Elapsed.TotalSeconds > 1)

{

controler.Reset();

counter++;

int cursorX = Cursor.Position.X;

int cursorY = Cursor.Position.Y;

previusForm.mainRichTextBox.AppendText((cursorX \* cursorY).ToString() + " ");

controler.Start();

BRNGMouseFormProgressBar.Value = counter;

}

if (counter > 9)

{

this.Close();

previusForm.Show();

}

}

Сама генерация в данном способе происходит при движении мыши по выделенному полю. Метод **mouseFormPictureBox\_MouseMove** срабатывает при передвижении мыши над изображением. Для генерации самого числа берется значение координат курсора мыши. Полученный результат так же отправляется **MainForm**.

private void BRNGMOUSEForm\_Load(object sender, EventArgs e)

{

MessageBox.Show("Shift the mouse to generate random numbers." , "Info", MessageBoxButtons.OK, MessageBoxIcon.Information);

}

Последний метод делает то же, что и в предыдущих формах, они показывают сообщение с описанием работы выбранного биологического генератора случайных чисел.

# **Заключение**

В данной курсовой работе было рассмотрено понятие случайных и псевдослучайных чисел, была представлена история развития понятия случайности и его влияние на жизнь человека. Были рассмотрены генераторы псевдослучайных чисел, а в частности биологический генератор случайных чисел.

В практической части курсовой работы была разработана и реализована программа, реализующая некоторые из способов работы биологического датчика случайных чисел.

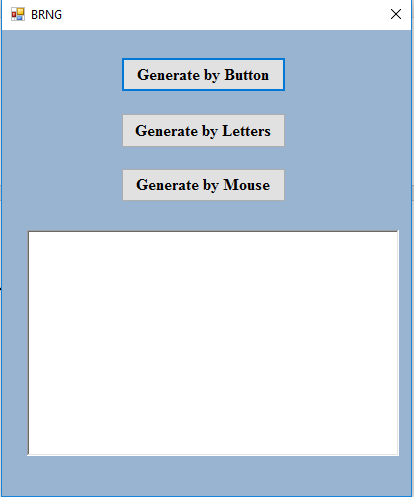
Подводя итог, хотелось бы сказать, что случайные числа играют важную роль в современном мире, они нашли свое применение во многих сферах и их генерация является насущной проблемой. Для решения данной проблемы были разработаны разнообразные аппаратные генераторы случайных чисел, но они не находят широкого применения из-за своей цены и необходимости встраивания в компьютер. С другой стороны, существуют генераторы псевдослучайных чисел, использующие разнообразные алгоритмы для генерации псевдослучайных последовательностей. Одним из них является биологический генератор случайных чисел. Он позволяет генерировать хорошие последовательности псевдослучайных чисел, но из-за времени генерации он не подходит для генерации большого количества чисел.

# **Cписок источников**

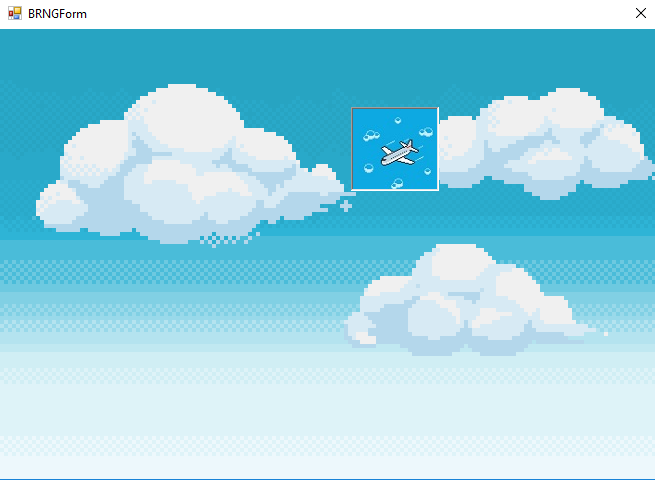
1. Брокгауз Ф.А., Ефрон И.А. Энциклопедический словарь Брокгауза и Ефрона в 82 тт. и 4 доп. тт. — М.: Терра, 2001 г. — 40 726 с.;
2. Harry F. ERNIE - A Random Number Generator [Электронный ресурс] - http://www.i-programmer.info/history/machines/6317-ernie-a-random-number-generator.html;
3. [Д. Кнут. Искусство программирования. Том 3](http://computersbooks.net/index.php?id1=4&category=teoriyaprogramirovaniya&author=shtona-v&book=20012) — Вильямс, 2001. — 788 c;
4. Д. Кнут. Искусство программирования. Том 2. Получисленные алгоритмы. — М.: Вильямс, 2000 —788с.;
5. Линейный конгруэнтный метод [Электронный ресурс] - http://www.intuit.ru/studies/courses/691/547/lecture/12383?page=2;
6. Д. Рихтер. CLR via C# Программирование на платформе Microsoft .Net Framework 4.5 на языке C#. 4-е изд. – СПБ.: Питер, 2016. – 896с.

# **Приложения**

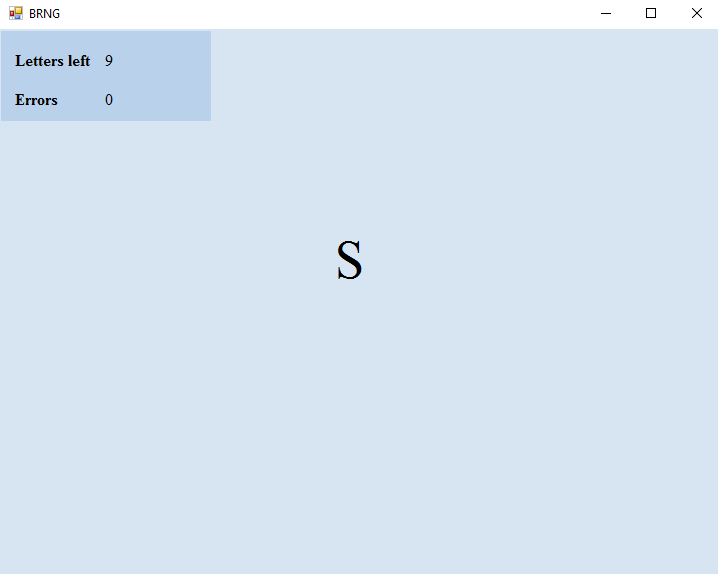
**Приложение А**



**Приложение Б**



**Приложение В**



**Приложение Г**

